CIO Information in the News

Summer '99 Volume IV Issue 3

INSIDE

Taking VA by Storm . 1
CIO Scene 2
Melissa!! 4
Interview with Bob Bubniak . . . 6
MDS Platform Installed 7
VHA Serves Veterans via Email 8
Advanced Process Asset Library . . . 8
VISTA Imaging . . . 9
One VA Conferences . . . 9
Access America for Senior Veterans . . 10
VBA Deploys Secure Internet Communications . . 10
Electronic Medical Debt Collection . 11
HR LINK$ Info Warehouse Migration 12
Hy Tech 12

TAKING VA BY STORM

By: Mike Donahue, OI&T Information Technology Support Service

Webster's Dictionary defines *bedlam* as "a place, scene, or state of uproar and confusion." Well, if you've ever experienced a "Message Storm" or "Mail Storm," you understand why it is referred to as *bedlam*. You probably also know that while the message storm is going on, it disrupts productivity system-wide.

A message storm can start simply--a user sends a single message to a large number of recipients. From this point things tend to happen quickly. Recipients grind the messaging system down by using *Reply to All* when responding. Frustrated by overflowing inboxes, recipients send *Reply to All* messages telling everyone to stop, which only causes the storm to swell.

Generally, one person sending a message to a large number of recipients does not cause a message storm. Storms are caused by the recipients inherent nature to "not want to be involved." People who would never consider sending a message to a large list of recipients don't hesitate to use *Reply to All* against the same list to send responses such as "Remove me from this list," or "Please quit Replying All to this message." And probably the worst possible contributor to a message storm is someone who sends a message with *Delivery* or *Read Receipts.* (These are affectionately called "The Kiss of Death" by system administrators.) If this type of message is sent, it leads to the worst kind of message storm, one that generates enormous floods of mail that swell exponentially.

In May 1999, the Department of Veterans Affairs email system was nearly brought to a grinding halt when faced with the ultimate worst-case scenario message storm. First, the original message started arriving throughout VA. Shortly thereafter came the *Reply to All* messages. Then, the nightmare of

(Continued on Page 2)

THE CIO SCENE

By: Harold F. Gracey, Jr., Acting VA Chief Information Officer

Let me be blunt. The Department's information security posture is not what it should be. Here are just three recent examples to support my assessment.

Friday, March 26, the Melissa virus first appeared on the world scene. Fortunately many (maybe most) VA facilities got an early enough alert that they were able to immunize their Exchange Email servers against the virus, and possibly to distribute to their end-users an updated desktop virus protection as well. In the week or so that followed, as word about this virus attack saturated the national news media, we should have expected our facilities to have completed a thorough prevention. Nevertheless, three months later, VA Central Office Exchange servers were still receiving Melissa-contaminated mail messages from one or more VA facilities around the country. This points to an imperfect response capability in VA to these worldwide threats. Unfortunately, because of the extent of connectivity across VA, "almost" is simply not good enough anymore.

In late May of this year, a junk Email storm (for want of a better name) was caused by the innocent act of just one employee. You, the reader, were probably inconvenienced by this event yourself. This incident easily cost VA over a million dollars in workforce disturbance, network interruptions, and technical clean-up over just a few days. It was a security matter because it gets to the heart of what is called "denial of service" in security program jargon. It followed on the heals of Melissa to dramatize how fragile to attack our network assets are, and the extraordinary costs that can result. Indeed, the research firm Computer Economics, Inc., estimated the costs to American businesses from virus attacks in just the first half of 1999 amount to $7.6 billion.

Earlier software tests of security vulnerabilities conducted by VA included statistical samplings of employee's "NT log-on user accounts" across several facilities. The results are appalling because they point to an institutional indifference by our workforce to each employee's obligations to information security. Almost 18,000 user accounts were sampled. About half of those accounts employed what is called a "weak" password, in other words a password that can easily be cracked using unsophisticated guessing techniques. More alarming is the fact that one in four of these accounts employed the default password for that facility's servers, the word "password", for instance. VA has much work to do on security awareness training, policy compliance measurement, and technical controls to fix this problem.

Audits by the General Accounting Office and VA's Inspector General the prior two years had already surfaced systemic vulnerabilities to our sensitive information because of years of under-investment and neglect. So our vulnerability is clearly Department-wide; and the incidents above only reinforce that point. The recent defacement and disruption to other agencies' Web sites point to an increased climate of threat to the Federal government's networks from many quarters, both domestic and foreign. How long VA will remain unharmed by a massive outside attack, or an information disclosure that is irreversibly damaging to its credibility, is anybody's guess. But we must all begin now to do our part individually and organizationally to improve our information security posture.

Taking VA by Storm

Continued from Page 1

someone sending a "Read Receipt" message was added to the equation. And if that wasn't enough of a problem, a couple of "High-Priority *Reply To All*" messages were thrown in for good measure. Bedlam had indeed come to VA!

What Happened. A single mail message was sent to the entire Global Address List (GAL) for VA. Let me reiterate… the **ENTIRE** Global Address List

for VA. This address list includes individual names as well as approximately 400 shared Distribution Lists (DLs). This means that John Smith not only receives the message because his name is in the GAL, he also receives a copy of the message every time his name is found in a DL.

Like many recipients, Mr. Smith deleted the first few messages he received, and proceeded with his daily work. Several hours and numerous repetitive messages later, Mr. Smith got fed up with all this mail and sent a *Reply to All* (instead of a reply to just the originator) requesting that his name be removed from the distribution list. Once other recipients began receiving Mr. Smith's message, they joined in the *Reply to All* party, requesting that their names also be removed from distribution. Because of the recent "Melissa" and "Papa" virus that impacted VA a short time ago, some recipients feared the message was a virus, and began sending *Reply to All* messages asking this question or cautioning other recipients about this possibility. So now the original message, the *Reply to All* messages, and the fear of a virus messages were circulating throughout VA nationwide. The message storm had reached gale force proportions. One individual sent a *Reply to All* message with a *Read Receipt* requested. (For those who don't know, a *Read Receipt* sends a notification back to the sender that their message has/has not been read.) Imagine the surprise (or horror!) of coming to work after a nice, relaxing weekend, opening your mail, and finding over 41,000 unread messages. That's right…41,000 unread messages!

By the time the Exchange Administrators started receiving the *Reply to All* messages, the message storm was already underway. Initially, we had no recourse but to let the storm wash over us. After several discussions with Microsoft technicians, however, utilities were provided to remove the original message and subsequent replies. Many long hours were spent manually checking server queues, mailboxes, and re-educating users who used the *Reply to All* feature. Within a week, the message storm had subsided. The VA email system is returning to normal operation with a few isolated incidents occurring as people return to work after periods of leave.

Lessons Learned. By following the suggestions outlined below, you can help prevent future message storms. Keep these tips handy and refer to them often!

1. When you receive an unwanted message, particularly when the message has been sent to an extremely large number of people, just delete it. By taking this simple action, you will contain a potential message storm.

2. If you cannot resist the urge to reply to one of these messages, limit your reply to the originator of the message. Do not use the *Reply to All* feature. When you choose *Reply to All*, you become part of the problem.

3. If you must send a reply to the originator, do not send it with high priority status. The Exchange system sends messages in order of priority. First HIGH, then MEDIUM, then LOW. As an Exchange Administrator, trust me when I tell you that the email system's HIGHEST PRIORITY is eliminating the message storm. Weighed against this criteria, your high priority message quickly becomes a low priority.

4. Do not request a read receipt. You don't want to log on to your email and find 41,000 mail messages in your Inbox, do you?

There are several preventive measures that can be taken at the network level in Central Office that would position us to respond more rapidly and effectively to message storms. We plan to implement them in the near future.

Distribution Lists would be limited exclusively to the recipients on the list. This would reduce user access to VACO lists, as well as prevent "outsiders" from *spamming* the list. *Spamming* is when a person or organization posts the same message many times on an email system. The problem is not the content of the message, but the fact that the message is everywhere, polluting the electronic landscape like an indiscriminate leaflet airdrop, instead of being sent just to the appropriate individual(s).

Mail delivery within the system would be limited to a prescribed number of users, for example 5,000. By setting this limit, anyone selecting the entire GAL in either the TO: or CC: fields would be inhibited after the first 5,000 recipients.

Read Receipts would be prohibited from use when sending a message to a large number of recipients.

Further corrective measures have been made available via the Microsoft Corporation. Technicians from Microsoft worked closely with VA Exchange Administrators in developing utilities that can remove *specific* messages from all users' mailboxes. With this utility, messages containing specific subject lines or having specific attachments can be pulled out of private mailboxes and retained, if necessary, outside the Exchange mail system. We applied this utility during the recent message storm to remove the original messages and the subsequent replies.

Another corrective tool developed by Microsoft removes specific messages from the Message Transfer Agent (MTA) queues. The MTA is a service that runs on Exchange servers and acts as the delivery agent between servers. The utility removes specific messages pending delivery to an Exchange server, thereby eliminating the messages prior to delivery to the user's mailboxes.

A sincere thanks to all the Exchange Administrators nationwide who battled the elements and helped us weather the storm! All is calm … for now.

Melissa!!

By: Michael Arant, VHA, Medical Information Security Service

March 26, 1999 was a day that the Medical Information Security Service (MISS) will long remember. It was a day that many in VA will remember. It was a day that profoundly changed our perspective on computer viruses.

MISS has lived with the world of computer viruses since the origin of the security program in 1987. The VHA security program grew in parallel with the evolution of viruses. As they arose, each new class of virus captured the imagination of the popular media and was advertised to the world as the next big threat to our information assets. However, our defensive measures grew in concert with viruses. Viruses, we learned through experience, were not a kind of electronic Armageddon, but annoyances and inconveniences. Their authors were kids spraying electronic graffiti. Defense against viruses became a cost of doing business. Indeed, since the emergence of an entire industry based on virus defense, our own collective overreaction against outbreaks has probably been just as disruptive as any viral payload. There were exceptions, but by and large, the few dangerous and damaging viruses were sporadic in their distribution and limited in their effect. Of the 40,000 or so different viruses "in the wild," there are only a few dozen that have all that it takes to be "effective," that is; bug-free, small, stealthy, dangerous, and most importantly highly replicative.

All that changed about 7 a.m. on March 26 when the Melissa virus was released on the world. Melissa passed through our electronic doorway several hours later. From there, innocent VA staff received and read Email messages and opened the attached Microsoft Word document. A "macro" within the document forwarded the message to 50 other people. Many of those recipients innocently forwarded the message. There followed an uncontrolled geometric progression of messages, like an electronic chain letter.

VA experienced what we call in the security business a "denial of service attack" on our Exchange

system. Denial of service attacks do not destroy data. They create conditions that bog down communications with useless processing functions. In Melissa's case, this useless function was the propagation of messages. The result of such an attack is the unavailability of those services we depend on to accomplish our mission. Any of you who were working late that day noticed the slowdown.

MISS became aware of the problem late Friday. The virus was merely hours old and no technical defense had yet been implemented. Telephone calls came through to MISS simultaneously from many VHA facilities, all describing receipt of Exchange messages with Microsoft Word attachments containing a list of pornographic web sites. These messages were usually reported as being from strangers. This activity seemed highly suspicious for viruses. Although we did not know it yet, antiviral software vendors had discovered it earlier that day and were developing a fix while we struggled to understand what we were witnessing.

VHA uses two main technical defenses against viruses: Trend's ScanMail for Exchange Email and Network Associates International's (NAI) VirusScan and NetScan. The NAI technical point of contact was called. He immediately informed us that VA was probably experiencing an attack by Melissa virus. He provided some background information and the first round of the software fix that they had just created a few hours earlier to deal with Melissa.

The Exchange Management Center (EMC) was contacted and we began working the two sides of the defense against Melissa. The EMC managed the Trend ScanMail component of VHA's antivirus response and MISS directed the NAI solution.

We immediately began compiling what we knew about Melissa and broadcasted a message with information about Melissa and a copy of the fix. This message was sent to available Exchange mailgroups representing security and systems management interests. By this time, MISS staff had received dozens of messages and the arrival rate of contaminated messages was increasing rapidly.

Within hours, the Trend ScanMail solution had been issued to sufficient numbers of Exchange servers to stop the geometric progression from facility to facility of these email messages and Melissa virus. By the next morning, the vast majority of these messages were free from viruses. ScanMail was working. Messages were being cleaned and were not producing additional rounds of email messages.

The ScanMail solution takes place at the enterprise level; it is VHA's "aerial defense." NAI, however, protects individual desktop computers and resource servers. In other words, to defeat Melissa, we had to use NAI software to go in "on the ground" and mop up those infected documents that ScanMail could reach. Unfortunately, that could not take place until ISOs and IRM staff read our messages and invoked the fix and we knew on Friday that probably would not take place until Monday morning!

Luckily, most facilities took the time to protect themselves. By protecting themselves, they reduced the risk to the entire enterprise. In the virtual world, we are indeed One VA; one undefended facility endangers all of us. Even now after a few weeks, there are sporadic outbreaks.

Just when we thought all was well, there emerged rumors of and reactions to a copycat virus, Papa virus. Luckily for us, Papa never passed through our doors. Interestingly, a rumor persists that Papa had a "bug" that prevented it from replicating reliably.

Later, Melissa had one more unpleasant surprise for VHA!

You see, Melissa has a second payload in addition to her ability to forward messages. When a desktop computer is infected (by an innocent victim's action of reading an infected document), Melissa will forward the NEXT document you open! This document can be a message from your hard drive that was never previously attached to a message. You can imagine the panic this has caused where anti-Melissa defense was not placed in service with the potential for breaches of privacy and negative public relations for all of VA.

There is a bright spot in this story. A suspect has been arraigned in this case. He stands accused of having released Melissa. After a decade of being victims of viruses, society is fighting back. Investigators have become savvy in the very technologies that virus writers have traditionally cowered behind. Our collective attitudes have changed. We are no longer content to see our resources compromised and our mission thwarted to feed the vanity of virus writers. It remains to be seen if judge and jury are willing to view attack on our information infrastructure in the same light as other crimes.

MISS is proud to have been in a position to help in defending VHA against this attack. We also wish to thank the EMC for their critical role of deploying the ScanMail fix. Most of all, we wish to thank those facility staff who took the time to deploy the VirusScan and NetScan fix on desktops and resource servers.

Michael Arant has been involved in the war against computer viruses in VHA for ten years. Ironically, he was a clinical microbiologist working with human viruses before joining the OCIO's information security team.

An Interview with Bob Bubniak

Robert P. Bubniak is Associate Deputy Assistant Secretary (ADAS) for Telecommunications in the Office of Information and Technology and has served in this position since October 25, 1998. As the ADAS, Mr. Bubniak plans, organizes, acquires and implements ubiquitous telecommunications programs and services for the Department. He is the chairman of the Interagency Management Council for Federal Telecommunications (IMC), a Federal Technology Service group comprised of telecommunications leaders from the cabinet agencies. The Council advises the Administrator of General Services on the management of all Federal telecommunications programs and policies.

What have been your major activities since arriving at VA?

I arrived to find that there were aggressive ongoing activities to find a replacement for the extant embedded Integrated Data Communications Utility (IDCU) wide area network. The contract was slated to terminate on May 31, 1999.

Bob Evans, under Harold Gracey's direction, was heading an IDCU Replacement Team and had the issues well in hand.

I determined to look to the future – to build coalitions and partnerships to improve communications and customer service. To assist in this endeavor, I moved the SAIC Project Manager (PM) for the IDCU from Virginia to my office suite and did the same with the Sprint PM. I also convinced AT&T that it was useful to provide an on-site representative to focus on FTS2000 issues. Dan Marsh of VHA provided an on-site FTS2000 Designated Agency Representative (DAR) which has helped to improve both communications and service.

Where do you see the telecommunications program going?

The telecommunications vision is evolutionary but it follows the One-VA model. It is: "To provide world class service to our veterans, their families and to the organizations we support via responsive, cost-effective telecommunications processes, to include managed network services."

What is Managed Network Services (MNS)?

MNS is a service which is expected to be provided by Sprint under the FTS2001 contract, the replacement for the IDCU contract. It will enable VA to benefit from Sprint's technological superiority in network management. Sprint manages global networks as their core business and we will be looking at the full spectrum of MNS—configuration management, performance management, fault management, monitoring, software management and hardware management to determine which of those offerings will best serve the needs of the Department. At present, we're working with Sprint to ensure timely migration from the private IDCU network to their public

network. As part of this plan, we intend to base line the network to identify choke points and opportunities for improving service.

Are there expected economies from the use of FTS2001?

We anticipate savings of at least 30 percent per year from the current voice and data costs and are also looking at staff realignments to maximize performance. We've started a program of providing Telecommunications Advisories which furnish insights on developments within the telecommunications milieu, such as FTS2001 pricing, which should help managers to plan their expenditures.

I see great opportunities to provide responsive, cost-effective voice, data and video service, and am optimistic about effecting a partnership with the Administrations, other customers and Sprint. This should lead to the successful implementation of exceptional telecommunications support in the future.

New Minimum Data Set (MDS) Platform Installed

By: Tom Crase, OI&T, Austin Automation Center

Veterans Health Administration (VHA) has a system, Patient Assessment File (PAF), at the Austin Automation Center (AAC) which processes batch data on assessments of patients' conditions. Over the years, this system has become inadequate in fulfilling VHA needs in this area. Rather than trying to expand the existing PAF system, a team from VHA made the determination that there is a need to acquire a more modern system which is database oriented and provides storage, access, and analysis of long-term care data on patients in VA facilities. Such a nationwide system Minimum Data Set (MDS) is in operation by the Department of Health and Human Services, Health Care Financing Administration (HCFA).

Through a contract between VHA and the vendor who developed MDS for HCFA, a hardware/ software solution was procured and installed at the AAC during the last week of April and first week of May 1999. The system consists of Quad Pentium Pro 200 MHz processors, 12 megabyte (MB) of memory, Compact Disk–Read Only Memory (CD-ROM), Small Computer System Interface (SCSI) 15/ 30 gigabyte (GB) Digital Linear Tape (DLT) tape drive, and five 4-GB hard drives configured with Redundant Array of Independent Disks (RAID)-1 (mirrored) for the operating system and RAID-0 (striped) for the database. This configuration will render approximately 12 GB of usable disk space for the database tables. The operating system is Windows New Technology (NT), the database server is Oracle, and connectivity to the system will be through VA's Intranet using a Web browser on the client side. The AAC will be supporting system and database administration tasks, backups, and a disaster recovery capability. In addition, the AAC is tasked with security and user administration tasks as well as customized queries to feed the Decision Support System (DSS), the Allocation Resource Center (ARC), and the National Patient Care Database (NPCD). Additional support tasks for the AAC are under negotiation at this time.

The system was installed and tested with two **V*IST*A** test sites, and system acceptance was made before the contractor departed. It will remain in test status supporting the implementation, training, and testing of the **V*IST*A** component, until national rollout which is scheduled for early calendar year 2000.

VHA Serves Veterans via Electronic Mail

By: Teresa Connelly, VHA National Patient Representative, and Walt Houser, OI&T, Information Management Service

America is making a major paradigm shift to the Internet, and veterans are no exception. During January 1 - March 31, 1999, Veterans Health Administration customer support staff handled 644 health related inquiries to VA web pages. The average response time was 2.1 days, including the time to reply to messages received on weekends and holidays.

There are times that a veteran's questions will not be answered on a web page. Nor is it pleasant or convenient to wait on hold on the telephone. Internet electronic mail provides our customers with the opportunity to ask their questions, then use their time on personal or business tasks. Electronic mail encourages more careful consideration of their question, as well as giving VA staff time to provide a precise and researched answer. While this means that an answer will not be immediately forthcoming, industry has found that customers are usually more willing to wait for an email reply than wait on hold for an extended period of time.

Of the veterans who identified their gender and era of service: 1% indicated they were female and 16% male; 5% indicated they were Gulf War veterans; 1% Korean; 4% Vietnam; and 4% WWII. The remaining gave no indication of their gender or era of service.

Seven percent (7%) of the inquiries were complimentary, including favorable remarks on visits to medical centers, the Web page, and services provided from the Web page. Sixty-five percent (65%) of the inquiries were neutral and of an informational nature. These requests covered a wide range of issues: Eligibility; Compensation and Pension; Request to Enroll via Homepage or Refill Prescriptions; Agent Orange; Information Regarding Employment; New Clinic Information and Nearest VA; CHAMPVA; Champus/Tri-Care; Filing a Claim for Service Connected Rating; Requests for Copies of Medical Records; E-Mail Addresses of Employees; Requests that need referals to other sources; Requests by students doing research.

Twenty-one percent (21%) involved complaints and samples include: VA Regional Office Complaints; Medical/Psychiatric Problem not Addressed; Requests for Specialized Treatment and Programs; Long Waits for Appointments; Medical Needs not Addressed; Requests for Medications not on the Formulary.

Seventeen percent (17%) of the inquiries involved contacting the Patient Advocate at the medical center in order to assist the inquirer.

Advanced Process Asset Library

By: Brandon Storms, OI&T, Austin Automation Center

In May 1999, the Austin Automation Center (AAC) developed and implemented the Advanced Process Asset Library (APAL) Web site. This is an interactive Web site that helps facilitate the integration of the Capability Maturity Model (CMM) into the AAC's software development process. The APAL Web site provides easy access to the processes, procedures, templates and forms found in the AAC's online Software Development Manual. Project team members use the Web site to help navigate through the requirements of each software project life cycle phase (e.g., requirements analysis phase, design phase, and code and unit test phase). Within each phase, the Web site provides a breakdown of all required and optional work products as well as a list of the roles and responsibilities of all team members. The Web site provides a variety of work product samples and templates, as well as a link to the Web-enabled Project Estimating Tool (PET) which team members can use to estimate the size, effort, and cost of all work products.

The APAL Web site is a proven success. The structured approach of the Web site has greatly improved communication between management, project team members, and especially AAC customers.

VISTA Imaging

By: Janis Sollenbarger, VHA, Implementation and Training Services

VISN 15 has taken the lead nationally through its innovative efforts to employ Vista Imaging in conjunction with telemedicine technology throughout its VISN.

Brian Belleau, VISN 15 telemedicine manager, has led these efforts supported by VISN management and many dedicated and progressive IRM and radiology staff members. Doug Wonnell, VISN 15 wide area network administrator, has worked closely with Mr. Belleau to facilitate VISN-wide image transfer in conjunction with their aggressive telemedicine programs. Mr. Belleau is in the final stages of implementing the hardware and network platforms at the individual medical centers to use the integrated Vista Imaging application. VISN 15 will be the first VISN to do so nationally. Mr. Belleau, with the assistance of the Silver Spring CIO Field Office technical support staff headed by Dr. Ruth Dayhoff and Janis Sollenbarger from Implementation and Training Services (ITS), is also beta testing the employment of teleradiology routing algorithms with the assistance of Dr. T. King at the Kansas City VA Medical Center. In addition to the core software applications associated with this product, this technology will "route" images taken at some VISN 15 medical centers to the VISN 15 Teleradiology Interpreting Center, enabling conservancy of higher paid specialists and enhancing patient care.

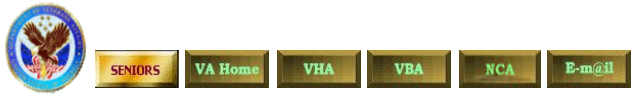
Use of the integrated Vista Imaging product is expected to provide for and enhance a continuum of care for VHA patients. The application integrates textual medical record information with clinical diagnostic images, such as radiology diagnostic images, non-radiology digital medical images, EKGs, scanned documents, and video conferencing transmissions, to provide for a truly comprehensive medical interpretation environment. In a recent example, Dr. Vincent L. Alvarez, chief medical officer for VISN 15, while at his desk at the network office, consulted with the Teleradiology Interpretation Center in Kansas City and a surgeon in Topeka while all were viewing the same CT image at the same time. Dr. Alvarez indicated that the availability of diagnostic images across the network "significantly raises the standard of care within the network."

Transmission of digital medical data bridges the geographical gaps to provide veterans with the best state-of-the-art comprehensive medical care. The employment of teleradiology and telemedicine technology, in conjunction with the integrated VistA Imaging application, affords all veterans the same high quality of care regardless of their physical location and proximity to specialists. Specialty consultations are no longer restricted to those veterans located in metropolitan medical center dominions.

Dr. Dayhoff's development team has been diligently working since 1990 to create the Vista Imaging application which has received international accolades for its unique and robust interface with the VHA's VistA health information system. These joint efforts – CIO and VISN 15 - will ensure that the veterans in VISN 15 receive the highest quality medical care available.

One VA Conferences

As VA becomes a leaner, more customer-focused organization, employees have broader opportunity and responsibility to learn to act as veteran advocates and to help remove walls between Administrations. The One VA conferences beginning in July 1999 are designed to stimulate that process through the development of action plans by teams comprising various VA organizations. Find out more about the regional conferences on the One VA Conference Website on VA's intranet home page vaww.va.gov



Access America for Senior Veterans

By: Walter Houser, OI&T, Information Management Service

VA's web site for senior veterans at http://www.va.gov/seniors/ is the Department's contribution to the National Performance Review for Government (NPRG) Access America for Seniors Project. With the involvement and cooperation of program offices across the Department, VA has worked together to use the latest in information technology to improve our service to veterans and their dependents, many of whom are senior citizens.

Key participants in the project are VHA's Geriatrics and Extended Care Strategic Healthcare Group (SHG), VBA's Loan Guaranty Service, the National Veterans Recreation Therapy Programs, and the Office of Planning and Analysis. Staff in the Office of Information and Technology (OI&T) designed and established the web site. Staff of the SHG and OI&T worked together to write web pages that promote quality care for aging and chronically ill veterans in the most efficient manner. Loan Guaranty specialists and OI&T staff developed web pages of Information for Elderly Homeowners. These pages cover reverse mortgages, interest rate reduction refinancing loans, and home equity fraud.

OI&T recruited the contributions of the National Veterans Recreation Therapy Programs, which is sponsoring with the Canandaigua VAMC the 13th National Veterans Golden Age Games. The Office of Planning and Analysis provided data on the estimated number of veterans living in the U.S. and Puerto Rico by age and period of service. To tie all these different sources into a One-VA common look and feel, staff of OI&T employed state-of-the-art technology that allows the entire 41-page seniors web site to be updated as a group yet maintained, as needed, by individual offices.

NPRG is looking for online transactions – to be able to apply for benefits, be approved, get the money and report back electronically. According to NPRG, delivering suites of completed electronic transactions tailored to seniors can completely transform their interaction with government.

VBA Deploys Secure Internet Communications

By: Dick Williams and Chris Elkington, VBA, Office of Information Management

The Veterans Benefits Administration (VBA) announced that it has implemented a state of the art Virtual Private Network (VPN) that will allow employees and accredited Veterans Service Organizations to access benefits information using the Internet.

The introduction of the VPN comes at an important time for VBA which is in the process of restructuring to better meet the challenges of providing needed services to our nation's veterans. As part of this effort, VBA, which has traditionally operated 58 regional offices, is rapidly expanding its service to centers located in local communities and military installations worldwide. These objectives would not be achievable without the cost effective, flexible and reliable communications provided by VPN. The secure communications provided by VPN will allow access to information from remote locations worldwide.

The VPN solution uses the public Internet to connect remote customers and staff to VBA's internal network. This new network, designed by Performance Engineering Corporation (PEC) of Fairfax, Virginia, is a unique systems solution. The VPN will provide a portable and secure means to send and receive data and to access the benefits applications required to provide expanded service to our nation's veterans.

Since the VPN uses a public network to carry private data, the VBA information exchange solution had to ensure the security of transmitted data. To provide security, PEC implemented a data encryption scheme that ensures that data cannot be accessed or tampered with by third parties while traveling over the Internet. VBA's VPN security is based on a "two-factor" authentication similar to Automated Teller Machines in the banking industry. A remote user attempting to access VBA resources through the VPN must provide a personal identification number (PIN) and a random number generated and displayed on a digital security device.

The VPN is a cost-effective information technology solution since it eliminates the need for VBA to maintain its own remote communications infrastructure. The VPN uses the resources of an Internet Service Provider-based network and common carriers like AT&T and Bell Atlantic, eliminating VBA's need to constantly procure, maintain, upgrade, or replace costly remote communications equipment.

Electronic First Party Medical Debt (Copayment) Collection

By: Jenifer Floyd, OI&T, Austin Automation Center

The Austin Automation Center (AAC) is working with Nations Bank in Atlanta, Georgia, and the Veterans Health Administration (VHA) to bring about a better system for the Department of Veterans Affairs to collect and process first party medical debt copayments. The formal name for the project is Consolidated Copayment Processing Center-Lockbox (CCPC-Lockbox); the more familiar name is simply "Lockbox." Progress points in the past six months are provided in this article.

Wilmington, Delaware, and San Antonio, Texas, VA medical centers (VAMCs) were eager to join Salem, Virginia, VAMC as Lockbox Phase 1 test sites. AAC staff worked with the bank and the centers to make this happen before the end of January. Phase 1 bank processing scans and makes an electronic record of VA remittance coupons and cash and check payments sent to the bank by patients of the three VAMCs. Quality assurance, workflow, and other essential procedures between the Lockbox and VA continue to be streamlined during this phase.

Working with the AAC's platform architect, VHA recently approved the acquisition of equipment and software for the Lockbox application. The platform will enable the AAC to deliver a robust application with online query and update components for use by VA Central Office (VACO) and the Financial Services Center (FSC), using a standard Web browser. Having knowledge of other VHA customer requirements, the AAC was able to incorporate Functional Status Outcomes Database (FSOD) platform requirements with Lockbox, resulting in a shared platform which reduces overall maintenance costs to VHA in future years.

The Lockbox Project Management Plan submitted by the AAC has been approved by the VACO Project Manager's office, and system requirements specifications have been distributed to the Lockbox Development Team. The Lockbox specifications call for providing distinct Lockbox (i.e., patient copayment financial data) functionality as well as providing for the integration of Lockbox data with other patient centric (patient care) data on VHA's National Patient Care Database (NPCD).

HR LINK$ Information Warehouse Migration to S/390 Enterprise Server at Austin

By: Nancy Edson, OI&T, Austin Automation Center

The Austin Automation Center (AAC) successfully migrated the production Human Resource (HR) LINK$ Information Warehouse (IW) to a new platform in mid-April. The IW is the HR employee self-service application that allows a VA employee to update various parts of his/her personnel record online through a kiosk workstation or through an interactive voice system. The IW has been available to the prototype sites for the past year, processing on a Digital Equipment Corporation (DEC) 4100 cluster with a Unix operating system and an Informix database. It now resides on the S/390 Enterprise Server running with the OS/390 operating system and DB2 database. Through a concerted team effort by personnel from the Shared Service Center (SSC) in Topeka, Kansas; VA Central Office; AAC; and IBM, the migration effort was completed on schedule and required a minimum amount of down time. The IW migration to the S/390 platform provides a cost-effective solution for the rollout of the IW to the entire VA employee community.

Hy Tech's Tip

By: Jay Anderson, OI&T, Technology Integration Service

There are several malicious software programs that can easily masquerade as automated greeting cards, jokes and gags. When you get one of these as an attachment to an email, be suspicious and refuse to open it. Opening it will execute it, if the file is an executable program file. Such a program can destroy the data on your system, install a computer virus or trojan horse program, or even install a remote administration program giving some remote and malicous person access to your system resources via the internet.

CIO Information in the News is published by the Office of Information and Technology to inform the VA IRM community of projects, activities, significant accomplishments, and upcoming events. You are invited to submit contributing articles. Please send your articles electronically to *CIO Newsletter*.

CIO Information in the News is available on the world wide web at www.va.gov/oirm/news/index.htm.

Editor: Kathy Ebel

Liaisons: OI&T - Chuck Fountaine
VHA - Cheryl Ludwa
NCS - Ella Demby
VBA - John Muenzen
BVA - Willie Alexander

WWW Support:
OI&T - Valerie Durkin